The Honorable Robert S. Lasnik

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff v. PAIGE A. THOMPSON, Defendant.	NO. CR19-159 RSL **UNITED STATES' OPPOSITION TO DEFENDANT'S MOTION TO COMPEL PRODUCTION OF CAPITAL ONE DATA**

I. INTRODUCTION

Defendant, Paige Thompson, is charged with hacking the hosted servers of dozens of companies and with downloading data that the victim companies stored on those servers. In addition to the other discovery that it has provided, the government has agreed to provide copies of the stolen data to the defense, with the exception of the data exfiltrated from one victim, Capital One Financial Corporation ("Capital One"). Capital One's data is subject to the Court's protection, because of the sensitive nature of data itself and because of the unique and virtually-unprecedented volume of data at issue. Specifically, the Capital One data set includes the personal identifiable information (PII) of more than 100 million Capital One customers - nearly one-third of America's population.

The government has made, and continues to make, the stolen Capital One data available for inspection at the FBI's secure facility. If, after inspecting the data, the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

defense identifies a smaller subset, or representative sample, of data that is actually material to the defense, the government will work with the FBI to provide a copy of that smaller sample to the defense, potentially in redacted form. But, the defense has not provided any credible explanation of why it needs a full copy of 100 million people's stolen PII. And creating a complete copy of this data for the defense inevitably would create some risk, no matter what steps were taken to protect the data, that it might be stolen or disseminated. Given the unique sensitivity of this data, the huge potential for harm to both Capital One and its customers if the data is stolen or disseminated, and the lack of materiality of the entire data set (as opposed to smaller representative samples of the complete data set), there is good cause to avoid creating and distributing new copies of the data. As a result, this Court should hold that the government has satisfied its discovery obligations and deny Thompson's motion to compel.

II. FACTS

The underlying facts of this case are outlined in Part II of the United States' Opposition to Defendant's Motion to Strike Cryptojacking Allegations and to Sever Count 8 (Docket No. 138), incorporated herein by reference. In brief summary, Thompson is charged with hacking servers maintained by Amazon Web Services ("AWS") and, among other things, stealing data of AWS clients that rented those servers. One of those clients was Capital One.

As shown in her social media posts, Thompson was well aware that the data that she had stolen included data from Capital One, and that this data included PII. Thompson also publicly threatened to disseminate the information. For instance, Thompson posted on Twitter:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

On July 26, 2019, shortly after being alerted to Thompson's crime by Capital One, the FBI obtained a search warrant for Thompson's residence and seized her computer. An FBI forensic computer scientist ("CS"), Waymon Ho, imaged and analyzed Thompson's computer. Among other evidence, CS Ho located stolen victim data, including Capital One data, in a file folder labeled "aws_hacking_shit/aws_scan." Importantly, the government believes it recovered the stolen data before Thompson disseminated it.

That data that Thompson stole from Capital One, and saved on her computer, included records relating to tens of millions of credit card applications and a smaller number of small business loan applications. The data contained PII, such as names, addresses, and dates of birth, of approximately 100 million individuals. They also included unencrypted Social Security numbers of a much smaller number of individuals, as well as tens of thousands of bank account numbers.

Following Thompson's arrest, the parties proposed, and the Court entered, a Protective Order governing discovery. *See* Protective Order (Docket No. 66). At the time that the parties proposed that order, they expressly discussed the fact that the government did not believe that the order adequately would protect the disclosure of the Capital One (and, perhaps, other) stolen data. As a result, the parties included in the protective order that they submitted to the Court, a provision that stated:

> In the event that the government believes that certain material should be made available for inspection, but should not be actually copied and produced even to the Defense

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

> Team (for example, because it contains particularly large volumes of PII or otherwise sensitive information), the government reserves the right to request that the Defense Team agree to such an arrangement, and, if the Defense Team does not agree, to raise the issue with the Court.

This provision was included in the Protective Order entered by the Court. *See* Protective Order ¶ 14. (Docket No. 66). (The parties also discussed the fact that this might not be an issue that ever needed to be addressed, if the case were resolved, as then appeared likely.)

The government subsequently produced voluminous discovery to Thompson. That discovery included images of Thompson's electronic devices, including the computer on which she had stored the stolen data. In producing the image of that computer, the government expressly and repeatedly stated, orally and in writing, that it had removed (and therefore was not producing) stolen victim data. *See, e.g.*, Andrew C. Friedman & Steven Masada, Letter to Muhammad Hamoudi, Christopher Sanders, Nancy Tenney, and Brian Klein (Feb. 10, 2020) (noting that the government "by agreement" had "remov[ed] obvious victim data" from the image). (A copy of this letter is attached as Exhibit A.)

In the summer of 2020, when it became clear that Thompson's case would not be resolved without a trial, Thompson's counsel requested a copy of the victim data stolen from Capital One and other entities. The Capital One data, which contains massively greater volumes of PII than that of any other victim in the case, posed particular concerns. Notably, too, Capital One, unlike any other victims in the case, objected to a full copy of the stolen data being created and provided to Thompson. (The government presumes that this is because Capital One was seeking to protect the individuals whose PII Thompson had stolen, and, perhaps also, because Capital One, which has incurred hundreds of millions of dollars in remediation costs, settlement costs, and civil regulatory penalties as a result of Thompson's breach, could face additional costs and penalties if the data were further disseminated.)

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The parties subsequently engaged in extensive discussions concerning means by which Thompson's counsel could have access to the stolen data. Among other options, the parties discussed having the data hosted on air-gapped computers (that is, computers not connected to the internet) in secure rooms at Capital One's counsel's offices in Seattle and any other city of Thompson's choice. They also discussed allowing Thompson's counsel and, their experts, unlimited access to these computers, and the ability to avoid having the identity of their experts, and the times and details of their review of the data, disclosed to the government. Thompson's counsel ultimately rejected this option.

Following the failure of the parties to reach agreement, Capital One sent a letter to the government invoking its rights under the Crime Victims' Rights Act and the Victims' Rights and Restitution Act and formally notifying the government that it objected to the government providing a complete copy of the stolen Capital One customer data to Thompson. *See* James Pastore, Letter to Andrew Friedman and Jessica Manca (Nov. 30, 1991). (A copy of this letter is attached as Exhibit B.)

III. ARGUMENT

Federal Rule of Criminal Procedure 16(a)(1)(E) requires the government to

> permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and
>
> (i) the item is material to preparing the defense;
> (ii) the government intends to use the item in its case-in-chief at trial; or
> (iii) the item was obtained from or belongs to the defendant.

Fed R. Crim. P. 16(a)(1)(E). This provision is, however, informed by another section of Rule 16, that is, Rule 16(d)(1), which grants the Court authority, "for good cause, [to] deny, restrict, or defer discovery or inspection, or grant other appropriate relief." Rule 16(d)(1) authorizes a court to limit disclosures otherwise required by Rule 16, when good

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

cause exists to do so. *United States v. Delia*, 944 F.2d 1010, 1018 (2d Cir. 1991). Good cause exists in this case.

Courts routinely are required to balance competing interests in determining whether a defendant is entitled to particular discovery. *See, e.g., United States v. Garcia*, 625 F.2d 162, 165 (7th Cir. 1980) (describing the decision to withhold disclosure of an informant's name as a "careful balance of competing interests" under Rule 16(d)(1)). Here, the Court must weigh the limited materiality of the data against the privacy interests of Capital One and the 100 million customers whose data Thompson stole.

A. Thompson Can Not Establish Materiality

When a defendant seeks discovery under Rule 16(a)(1)(E)(i), the defendant must make a threshold showing of materiality. *United States v. Santiago,* 46 F.3d 885, 894 (9th Cir. 1995). Materiality is shown by "facts which would tend to show that the Government is in possession of information helpful to the defense." *Id.* (*quoting United States v. Mandel,* 914 F.2d 1215, 1219 (9th Cir. 1990)). "Neither a general description of the information sought nor conclusory allegations of materiality suffice." *Id.*

Thompson has not articulated any reason why she requires a complete copy of the data stolen from Capital One, or how having a complete copy of this information would be helpful to the defense. The fact that Thompson stole 100 million records is simply not material to the case. Thompson would be equally liable for any of the crimes with which she is charged had she stolen one million, or even a mere thousand, records from Capital One.

In addition, the materiality of the full data set is rebutted by the apparent nature of Thompson's defense. It does not appear that attribution and identity are at issue. The Capital One data was recovered from Thompson's computer, in her bedroom, and Thompson admitted that she downloaded it. It is also clear from social media records that Thompson looked at the data and knew that it included PII. *See* Tweet, at page 2, *supra* (recognizing that "[t]here ssns . . . with full name and dob").

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Rather, if the defense pretrial motions are any indication of the defense theory, the central issues in the case will be Thompson's method of accessing the protected computers and her state of mind. The fact that the Capital One data set includes names, dates of birth, social security numbers, and bank account numbers bears on Thompson's intent, but that fact that the stolen data includes 100 million lines of individual victim PII does not.

In addition to her inability to establish that it is material for her to receive the full set of 100 million records containing victims' PII, Thompson also cannot establish that the data is covered by either of the other prongs of Rule 16(a)(1)(E). Although the government will prove Thompson's theft of Capital One data in its case-in-chief, the government does not intend to offer 100 million people's names, birthdates, addresses, and credit histories in evidence at trial. *See* Fed. R. Crim. P. 16(a)(1)(E)(ii). Rather the government will introduce file directories (that is, lists of files), which have already been produced to the defense, and small, redacted, representative examples of the stolen data entries. Thompson also obviously cannot establish that the data at issue belongs to her, since she stole it from Capital One. *See id.* 16(a)(1)(iii).

B. The Victims Have a Strong Privacy Interest.

Although Thompson does not have a substantial interest in obtaining a full set of the stolen data, the 100 million people whose PII Thompson stole have a compelling privacy interest that would be implicated if Thompson were provided a complete set of the stolen data. *See*, *e.g., Haber v. Evans,* 268 F. Supp. 2d 507, 512 (E.D. Pa. 2003) (recognizing, in the context of a newspaper's request for court records, the privacy interests of non-public persons named in a law enforcement misconduct investigation).

That interest can be partially protected by the existing Protective Order, which prohibits the defense from copying protected material or sharing it beyond the defense team. But, only partially so. Creating an additional copy of the PII introduces an inevitable risk of dissemination. The government has no doubt defense counsel would take great precautions with the information, but we live in an age in which no defense is

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

impermeable to cybercriminals. Recent history is replete with examples of cybercrime by nation states, by foreign hackers, and by disgruntled employees. And, the victims regularly include institutions that take great precautions to protect data, agencies involved in national security and leading technology corporations.

Even the principal measure that defense counsel propose to protect the data – storing the data on an air gapped computer - is no guaranty of security. Air gapped computers, like any other, can be hacked. *See, e.g.,* 'Air-Fi' attack renders air-gapped computers open to data exfiltration through WiFi signals, https://portswigger.net/daily-swig/air-fi-attack-renders-air-gapped-computers-open-to-data-exfiltration-through-wifi-signals (last visited December 29, 2021). Put simply, no entity - including the Federal Public Defender - is immune from cybercrime.

The risk here is magnified by the volume of the information. The information Thompson stole, and of which she now requests a copy, is one of the largest troves of PII ever stolen by a cybercriminal. Even if the chance of dissemination is small, the risk is amplified by the sheer volume of information at stake. Further dissemination of the stolen information in this case would harm the 100 million individuals whose PII is involved - a massive number of potential victims. The harm to them includes the fact that, if their PII were disseminated (as Thompson threatened to do), these victims' privacy would be violated. It also includes a clear risk that the 100 million victims would be subject to identity theft, a crime that often imposes much greater harm and costs on victims than traditional financial crimes.

Providing a complete copy of the stolen data to Thompson's counsel also would harm Capital One. As previously noted, Capital One has asserted its rights under the Crime Victims' Rights Act and the Victims' Rights and Restitution Act. *See* Exhibit B. Among other rights, these acts give Capital One the right to be reasonably protected from the accused and to be treated with fairness and respect for its dignity and privacy. *See* 18 U.S.C. § 3771(a)(1), (8). Thompson's actions already have cost Capital One hundreds of millions of dollars in

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

remediation costs, legal settlements, and regulatory penalties. Further dissemination of the stolen information would risk causing further substantial financial harm to the company, as well as to its customers.

C. The Government's Proposed Course Balances Thompson's and Victims' Interests

The government has offered Thompson's counsel a path forward that satisfies Thompson's right to discovery, while respecting the weighty privacy interests involved in this case. Under the government's proposal, Thompson's representatives would first view the information stolen from Capital One at the FBI. (To the extent that Thompson wishes to preserve the secrecy of her testifying expert at trial, Thompson could retain or send a different person to do this.)

Although, it serves no purpose for Thompson's defense to obtain a copy of 100 million records stolen from Capital One, and saved in a format that presumably reflects nothing more than the file structure under which they were stored by Capital One, to the extent that Thompson's representatives determine that it would be helpful for Thompson's defense to obtain a reasonable representative sample of data material, the government will provide Thompson's counsel a copy of that data, possibly in redacted form. Limiting the data that is copied will minimize the possible risk of a subsequent massive dissemination of victim PII.

This solution appropriately balances the competing interests in the case. It allows Thompson's counsel to view all of the data in the case, and to obtain a copy of more limited data that is actually material. As a result, it allows Thompson's counsel vigorously and effectively to defend Thompson. But, it also recognizes, and limits, the unique risk of further dissemination, and injury to victims, resulting from the massive volumes of PII in this case.

Notably, this solution also is consistent with the approach taken in at least one other significant case. In *United States v. Pacific Gas & Electric Co.,* 2015 U.S. Dist. LEXIS 84139, at *39 (N.D. Ca. 2015), defendants sought copes of all of the government's witness interview notes. The government declined to provide copies of a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

full set of the notes, but offered to make them available for review, and to copy those notes that Pacific Gas & Electric wished to use at trial. *See id.* at *39-41. The court rejected the defense's broad claim that this would mean the notes were not readily available to the defense for trial preparation, and it found that the government's offer was sufficient to comply with Rule 16. *See id.* at 41. That is even more clearly the case here: the material at issue, which includes 100 million peoples' PII, is more deserving of protection than the interview notes at issue in *Pacific Gas & Electric*, and the value to the defense of having a full 100-million record set of the actual data is minimal as compared to that of a complete set of interview notes.[1]

IV. CONCLUSION

For the foregoing reasons, the Court should find that the government has reasonably complied with its discovery obligations in making the Capital One data available for inspection, and by offering to provide actual copies of a limited volume of

//

//

//

[1] Although *Pacfic Gas & Electric* was decided under Federal Rule of Criminal Procedure 16(a)(1)(B), which requires the government to make materials "available for inspection, copying, *or* photographing" (emphasis added), rather than Rule 16(a)(1)(E), which requires the government to "permit the defendant to inspect *and* to copy . . . data" (emphasis added), the Court can and should approve the same procedure in the present case, based upon the strengths of the interests involved, and pursuant to Rule 16(d)(1), which expressly allows the Court "for good cause, [to] deny, restrict, or defer discovery or inspection, or grant other appropriate relief."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information that is actually material to Thompson's defense. As a result, the Court should deny Thompson's motion to compel.

DATED: December 29, 2021.

Respectfully submitted,

NICHOLAS W. BROWN
United States Attorney

/s/ Andrew C. Friedman

ANDREW C. FRIEDMAN
JESSICA M. MANCA
Assistant United States Attorney
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
Telephone: (206) 553-7970
Fax: (206) 553-0882
E-mail: Andrew.Friedman@usdoj.gov
Jessica.Manca@usdoj.gov